The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/22/20

SUBJECT:
A Vulnerability with Cisco Adaptive Security Appliance and Firepower Threat Defense Could Allow for Denial of Service

OVERVIEW:
A vulnerability has been discovered in Cisco Adaptive Security Appliance and Firepower Threat Defense, which could allow for a denial of service condition. Cisco Adaptive Security Appliance is the core operating system that delivers enterprise-class firewall capabilities and Cisco Firepower Threat Defense is an integrative software image. Successful exploitation of this vulnerability could allow an attacker to cause denial-of-service condition.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Cisco Adaptive Security Appliance prior to 9.12.4.2
- Cisco Adaptive Security Appliance prior to 9.13.1.12
- Cisco Adaptive Security Appliance prior to 9.14.1.9
- Cisco Firepower Threat Defense Software prior to 6.4.0.9
- Cisco Firepower Threat Defense Software prior to 6.6.0.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Cisco Adaptive Security Appliance and Firepower Threat Defense, which could allow for a denial of service condition due to a memory-exhaustion condition. Specifically, this issue occurs when processing certain TCP packets. An attacker can

exploit this issue by sending a high rate of specially-crafted TCP traffic through an affected device. Successful exploitation of this vulnerability could allow an attacker to cause denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Cisco to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-QFcNEPfx

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3554